

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-20. (Cancelled)

21. (Previously presented) A system comprising:  
a network;  
a security operation center coupled with the network; and  
one or more machines coupled with the network, each machine comprising a  
communication interface and a memory including an execution area configured to perform  
operations comprising examining a set of instructions embodying an invoked application to  
identify the invoked application, obtaining application-specific intrusion criteria, and monitoring  
network communications for the invoked application, after the examining and the obtaining,  
using the application-specific intrusion criteria to detect an intrusion.

22. (Original) The system of claim 21, wherein the application-specific intrusion criteria  
comprises a normal communication behavior threshold.

23. (Original) The system of claim 21, wherein the application-specific intrusion criteria  
comprises an intrusion signature.

24. (Original) The system of claim 21, wherein monitoring network communications  
comprises monitoring network communications in a network intrusion detection system  
component running in an execution context with the invoked application.

25. (Original) The system of claim 24, wherein the operations further comprise providing an application-specific remedy for a detected intrusion.

26. (Original) The system of claim 25, wherein providing an application-specific remedy comprises cutting at least a portion of the network communications for the invoked application.

27. (Original) The system of claim 24, wherein each machine further comprises a local repository, the security operation center includes a master repository, and wherein obtaining the application-specific intrusion criteria comprises:

requesting the application-specific intrusion criteria from the local repository;

requesting the application-specific intrusion criteria from the master repository if the application-specific intrusion criteria is unavailable in the local repository;

receiving the application-specific intrusion criteria from the master repository if requested; and

receiving the application-specific intrusion criteria from the local repository.

28. (Original) The system of claim 24, wherein examining the set of instructions comprises:

applying a hash function to the set of instructions to generate a condensed representation; and

comparing the condensed representation with existing condensed representations for known applications.

29-30. (Cancelled)